PPP-Authentifizierung mit dem PPP-chap-Hostnamen und den ppp-Authentifizierungschap-Callin-Befehlen

Inhalt

Einführung

Die PPP-Aushandlung umfasst mehrere Schritte, z. B. die Verhandlung über das Link Control Protocol (LCP), die Authentifizierung und die NCP-Aushandlung (Network Control Protocol). Wenn sich die beiden Seiten nicht auf die richtigen Parameter einigen können, wird die Verbindung beendet. Sobald die Verbindung hergestellt ist, authentifizieren sich die beiden Seiten anhand des bei der LCP-Aushandlung festgelegten Authentifizierungsprotokolls. Die Authentifizierung muss erfolgreich sein, bevor die NCP-Aushandlung gestartet wird.

PPP unterstützt zwei Authentifizierungsprotokolle: Password Authentication Protocol (PAP) und Challenge Handshake Authentication Protocol (CHAP).

Voraussetzungen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Anforderungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den unten stehenden Software- und Hardwareversionen.

- Cisco IOS® Softwareversion 11.2 oder höher

Hintergrundtheorie

Die PAP-Authentifizierung umfasst einen bidirektionalen Handshake, bei dem Benutzername und Kennwort im Klartext über den Link gesendet werden. Daher bietet die PAP-Authentifizierung keinen Schutz vor Wiedergabe und Zeilenausschnitt.

Die CHAP-Authentifizierung dagegen überprüft regelmäßig die Identität des Remote-Knotens mithilfe eines Drei-Wege-Handshake. Nachdem die PPP-Verbindung hergestellt wurde, sendet der Host eine "Herausforderung"-Nachricht an den Remote-Knoten. Der Remoteknoten reagiert mit einem Wert, der mit einer unidirektionalen Hashfunktion berechnet wird. Der Host überprüft die Antwort anhand seiner eigenen Berechnung des erwarteten Hashwerts. Wenn die Werte übereinstimmen, wird die Authentifizierung quittiert. Andernfalls wird die Verbindung beendet.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das IOS-Befehlssuche-Tool.

Konfigurieren der unidirektionalen CHAP-Authentifizierung

Wenn zwei Geräte normalerweise die CHAP-Authentifizierung verwenden, sendet jede Seite eine Herausforderung, auf die die andere Seite reagiert und die vom Herausforderer authentifiziert wird. Jede Seite authentifiziert sich unabhängig voneinander. Wenn Sie mit Routern von Drittanbietern arbeiten möchten, die keine Authentifizierung durch den anrufenden Router oder das anrufende Gerät unterstützen, müssen Sie den Befehl **ppp authentication chap callin** verwenden. Wenn der Befehl **ppp authentication** mit dem **callin**-Schlüsselwort verwendet wird, authentifiziert der Access Server das Remote-Gerät nur, wenn das Remote-Gerät den Anruf initiiert hat (z. B., wenn das Remote-Gerät "eingewählt" wurde). In diesem Fall wird die Authentifizierung nur für eingehende (empfangene) Anrufe angegeben.

Konfigurieren eines anderen Benutzernamens als des Routernamens

Wenn ein entfernter Cisco Router mit einem zentralen Router von Cisco oder einem Router einer anderen Verwaltungskontrolle, einem Internet Service Provider (ISP) oder einem Router von zentralen Routern verbunden ist, muss ein Benutzername für die Authentifizierung konfiguriert

werden, der sich vom Hostnamen unterscheidet. In diesem Fall wird der Hostname des Routers nicht angegeben oder ist zu unterschiedlichen Zeiten (rotierend) unterschiedlich. Der Benutzername und das Kennwort, die vom ISP zugewiesen werden, sind möglicherweise nicht der Hostname des Remote-Routers. In einer solchen Situation wird der Befehl **ppp chap hostname** verwendet, um einen alternativen Benutzernamen für die Authentifizierung anzugeben.

Stellen Sie sich beispielsweise eine Situation vor, in der sich mehrere Remote-Geräte an einem zentralen Standort einwählen. Unter Verwendung der normalen CHAP-Authentifizierung muss der Benutzername (der Hostname) jedes Remote-Geräts und ein gemeinsam genutzter geheimer Schlüssel auf dem zentralen Router konfiguriert werden. In diesem Szenario kann die Konfiguration des zentralen Routers langwierig und umständlich sein. Wenn die Remote-Geräte jedoch einen Benutzernamen verwenden, der sich von ihrem Hostnamen unterscheidet, kann dies vermieden werden. Der zentrale Standort kann mit einem einzigen Benutzernamen und einem gemeinsamen geheimen Schlüssel konfiguriert werden, der zur Authentifizierung mehrerer Wählclients verwendet werden kann.

Netzwerkdiagramm

Wenn Router 1 einen Anruf bei Router 2 initiiert, fordert Router 2 Router 1 an, Router 1 jedoch nicht Router 2. Dies liegt daran, dass der Befehl **ppp authentication chap callin** auf Router 1 konfiguriert ist. Dies ist ein Beispiel für eine unidirektionale Authentifizierung.

In dieser Konfiguration wird der Befehl **ppp chap hostname alias-r1** auf Router 1 konfiguriert. Router 1 verwendet "alias-r1" als Hostnamen für die CHAP-Authentifizierung statt "r1". Der Name der Wählzuordnung für Router 2 muss mit dem Hostnamen der PPP-Karte von Router 1 übereinstimmen. Andernfalls werden zwei B-Kanäle eingerichtet, einer für jede Richtung.

Konfigurationen

Router 1

```
!
 isdn switch-type basic-5ess
 !
 hostname r1
 !
 username r2 password 0 cisco
 ! -- Hostname of other router and shared secret !
interface BRI0/0 ip address 20.1.1.1 255.255.255.0 no ip
directed-broadcast encapsulation ppp dialer map ip
20.1.1.2 name r2 broadcast 5772222
  dialer-group 1
  isdn switch-type basic-5ess
  ppp authentication chap callin
 ! -- Authentication on incoming calls only  ppp chap
hostname alias-r1
 ! -- Alternate CHAP hostname ! access-list 101 permit
```

```
ip any any dialer-list 1 protocol ip list 101 !
```

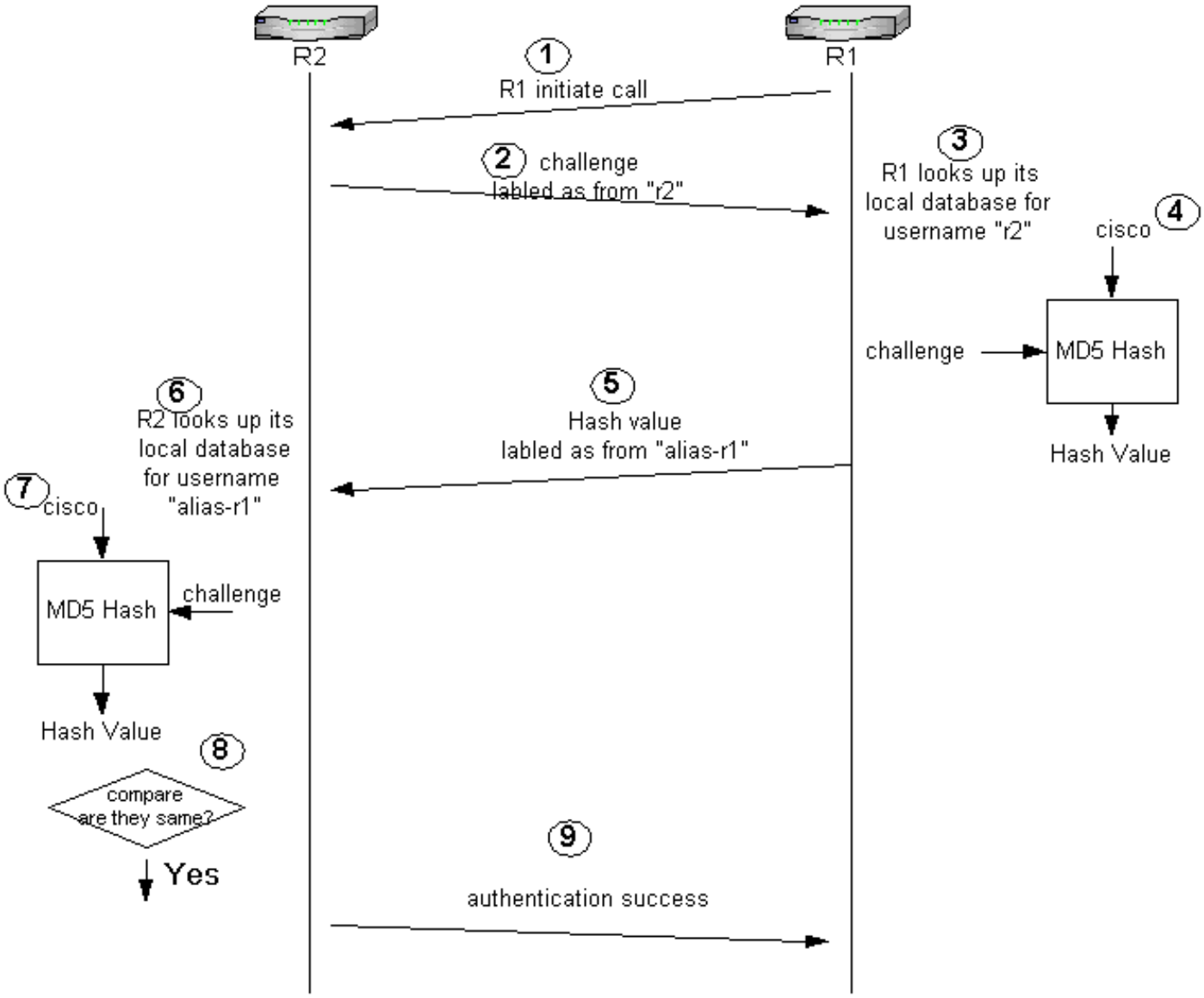
Router 2

```
!
 isdn switch-type basic-5ess
 !
 hostname r2
 !
 username alias-r1 password 0 cisco
  ! -- Alternate CHAP hostname and shared secret. ! --
The username must match the one in the ppp chap hostname
! -- command on the remote router.

 !
 interface BRI0/0
  ip address 20.1.1.2 255.255.255.0
  no ip directed-broadcast
  encapsulation ppp
  dialer map ip 20.1.1.1 name
  alias-r1 broadcast 5771111
   ! -- Dialer map name matches alternate hostname
"alias-r1". dialer-group 1 isdn switch-type basic-5ess
ppp authentication chap ! access-list 101 permit ip any
any dialer-list 1 protocol ip list 101 !
```

Erläuterung der Konfiguration

Erklärungen hierzu finden Sie in der folgenden Grafik:



1. In diesem Beispiel initiiert Router 1 den Anruf. Da Router 1 mit dem Befehl **ppp authentication chap callin** konfiguriert ist, wird der anrufende Teilnehmer, d. h. Router 2, nicht angegriffen.
2. Wenn Router 2 den Anruf empfängt, wird Router 1 zur Authentifizierung angegriffen. Standardmäßig wird bei dieser Authentifizierung der Hostname des Routers verwendet, um sich selbst zu identifizieren. Wenn der Befehl **ppp chap hostname konfiguriert ist, verwendet ein Router den Namen anstelle des Hostnamens, um sich selbst zu identifizieren.** In diesem Beispiel wird die Herausforderung als "r2" bezeichnet.
3. Router 1 empfängt die Herausforderung von Router 2 und sucht in der lokalen Datenbank nach dem Benutzernamen "r2".
4. Router 1 sucht das "r2"-Kennwort, d. h. "cisco". Router 1 verwendet dieses Kennwort und die Herausforderung von Router 2 als Eingabeparameter der MD5-Hash-Funktion. Der Hashwert wird generiert.
5. Router 1 sendet den Hash-Ausgabewert an Router 2. Da hier der Befehl **ppp chap hostname** als "alias-r1" konfiguriert ist, wird die Antwort als von "alias-r1" kommend gekennzeichnet.
6. Router 2 empfängt die Antwort und sucht in der lokalen Datenbank nach dem Benutzernamen "alias-r1" für das Kennwort.
7. Router 2 stellt fest, dass das Kennwort für "alias-r1" "cisco" lautet. Router 2 verwendet das Kennwort und die zuvor an Router 1 gesendete Herausforderung als Eingabeparameter für die MD5-Hash-Funktion. Die Hashfunktion generiert einen Hashwert.

8. Router 2 vergleicht den von ihm generierten Hashwert mit dem von Router 1 empfangenen Hashwert.
9. Da die Eingabeparameter (Herausforderung und Kennwort) identisch sind, ist der Hashwert gleich, was zu einer erfolgreichen Authentifizierung führt.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Bevor Sie einen der Debugbefehle ausprobieren, lesen Sie die Informationen Wichtige Informationen über Debugbefehle.

Beispielausgabe für Debugging

Das nachfolgende Beispiel zeigt die Ausgabe des Befehls **debug ppp authentication**:

Router 1

```
r1#ping 20.1.1.2

 Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 20.1.1.2, timeout is 2 seconds:

  *Mar 1 20:06:27.179: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
  *Mar 1 20:06:27.183: %ISDN-6-CONNECT:
  Interface BRI0/0:1 is now connected to 5772222
  *Mar 1 20:06:27.187: BR0/0:1 PPP: Treating connection as a callout
  *Mar 1 20:06:27.223: BR0/0:1 CHAP: I CHALLENGE id 57 len 23 from "r2"
   ! -- Received a CHAP challenge from other router (r2) *Mar 1 20:06:27.223: BR0/0:1 CHAP:
Using alternate hostname alias-r1
  ! -- Using alternate hostname configured with ! -- ppp chap hostname command *Mar 1
20:06:27.223: BR0/0:1 CHAP: O RESPONSE id 57 Len 29 from "alias-r1" ! -- Sending response from
"alias-r1" ! -- which is the alternate hostname for r1 *Mar 1 20:06:27.243: BR0/0:1 CHAP: I
SUCCESS id 57 Len 4 ! -- Received CHAP authentication is successful ! -- Note that r1 is not
challenging r2 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 36/38/40 ms r1#
*Mar 1 20:06:28.243: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to
up r1# *Mar 1 20:06:33.187: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5772222 r2
```

Router 2

```
r2#

  20:05:20: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
  20:05:20: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5771111
  20:05:20: BR0/0:1 PPP: Treating connection as a callin
  20:05:21: BR0/0:1 CHAP: O CHALLENGE id 57 Len 23 from "r2"
  ! -- r2 is sending out a challenge 20:05:21: BR0/0:1 CHAP: I RESPONSE id 57 Len 29 from
"alias-r1"
 ! -- Received a response from alias-r1, ! -- which is the alternate hostname on r1 20:05:21:
```

```
BR0/0:1 CHAP: O SUCCESS id 57 Len 4 ! -- Sending out CHAP authentication is successful 20:05:22:
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to up 20:05:26: %ISDN-6-
CONNECT: Interface BRI0/0:1 is now connected to 5771111 alias-r1
```

Zugehörige Informationen

- PPP-Befehle für Wide Area Networking
- PPP- und PPP-Authentifizierung im Überblick
- ISDN-Debugging-Informationen